Séminaire Dubreil.
Algèbre et théorie
des nombres

M. Lazard

Groupes de Lie formels à un paramètre

Séminaire Dubreil. Algèbre et théorie des nombres, tome 8 (1954-1955), exp. nº 5 et 7, p. 1-31

<http://www.numdam.org/item?id=SD_1954-1955__8__A3_0>

© Séminaire Dubreil. Algèbre et théorie des nombres
(Secrétariat mathématique, Paris), 1954-1955, tous droits réservés.

L'accès aux archives de la collection « Séminaire Dubreil. Algèbre et théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Exposés n° 5 et 7

GROUPES DE LIE FORMELS A UN PARAMÈTRE

(Exposés de M. Lazard, les 6 et 20 décembre 1954)

-:-:-:-:-

1.- Notions générales.-

Nous utiliserons la définition et les propriétés des séries formelles qui sont exposées dans l'Algèbre de Bourbaki (Chap.IV, paragraphe 5). Nous nous écarterons cependant légèrement des notations de cet auteur en ne considérant que des séries formelles dont le terme constant est nul, et en désignant, par exemple, par $K[[x,y]]$ l'anneau des séries formelles en x et y, sans terme constant, à coefficients dans l'anneau commutatif et avec unité K. Cette convention nous permettra de substituer dans tous les cas des séries formelles aux indéterminées figurant dans une série formelle.

C'est ainsi que, si $f(x,y) \in K[[x,y]]$, nous poserons :

$$(1.1) \qquad \Gamma f(x,y,z) = f(f(x,y),z) - f(x,f(y,z)) .$$

Si f et g sont deux séries formelles (ayant mêmes indéterminées et même anneau des coefficients), nous conviendrons d'écrire :

$$(1.2) \qquad f \equiv g \quad (\text{mod.deg.}q)$$

pour indiquer que f et g ne diffèrent que par des monomes de degré total au moins égal à q (entier positif). Par exemple, si $f = \sum_{i,j} a_{i,j} x^i y^j$, $g = \sum_{i,j} b_{i,j} x^i y^j$, la relation (1.2) signifie que $a_{i,j} = b_{i,j}$ pour tout couple (i,j) tel que $i + j < q$.

Nous dirons qu'une série formelle $f(x,y) \in K[[x,y]]$ est une loi de groupe à coefficients dans K si elle vérifie :

$$(1.3) \qquad \begin{cases} \text{a)} & f(x,y) \equiv x + y \qquad (\text{mod.deg.}2) \\ \text{b)} & \Gamma f(x,y,z) = 0 \ . \end{cases}$$

Si nous considérons un anneau A de séries formelles sur K, la donnée d'une loi de groupe $f(x,y)$ permet d'y définir une structure de groupe en posant $u \ast v = f(u,v)$ pour tous $u,v \in A$. En effet; l'opération $\ast$ est associative d'après (1.3.b), et les équations $t \ast u = v$ et $u \ast t = v$ sont résolubles en t pour tous $u,v \in A$, d'après (1.3.a). On vérifie facilement que l'élément neutre est 0, ce qui donne, comme conséquence de (1.3.a) et (1.3.b) :

$$(1.3.c) \qquad f(0,x) = f(x,0) = x \ .$$

Nous dirons qu'une loi de groupe $f(x,y)$ est <u>abélienne</u> si $f(x,y) = f(y,x)$.

<u>Théorème 1</u>.- Si l'anneau K n'a pas d'éléments nilpotents, toute loi de groupe à coefficients dans K est abélienne.

<u>Démonstration</u> : Nous nous appuierons sur une identité de Philip Hall qui constitue l'équivalent, pour les groupes, de l'identité de Jacobi pour les algèbres de Lie.

Si G est un groupe noté multiplicativement, nous poserons $(x,y) = xyx^{-1}y^{-1}$ et $x^y = yxy^{-1}$ pour tous $x, y \in G$. L'identité de Hall est alors :

$$((x,y),z^y)((y,z),x^z)((z,x),y^x) = e \quad (\text{élément neutre de } G) \ .$$

Elle se vérifie directement en écrivant un " mot " de 42 lettres qu'on supprime ensuite les unes après les autres dans un ordre convenable.

Soit $f(x,y)$ une loi de groupe à coefficients dans l'anneau K. L' "inverse formel" $g(x)$ de x est la série formelle qui vérifie $f(x,g(x)) = f(g(x),x) = 0$. Puisque $f(x,y) = x + y$ (mod.deg.2), nous avons $g(x) = -x$ (mod.deg.2), et $g(x) = -x + \sum_{i=2}^{\infty} b_i x^i$. Pour simplifier l'écriture, nous poserons comme précédemment $f(x,y) = x \ast y$.

Les analogues "formels" des notations multiplicatives x^y et (x,y) sont alors deux séries formelles en x et y :

$$k(x,y) = y \ast x \ast g(y) \quad \text{et} \quad h(x,y) = x \ast y \ast g(x) \ast g(y) \ .$$

Si nous faisons opérer la loi de groupe $f(x,y)$ sur un anneau de séries formelles, nous voyons que f est abélienne si et seulement si $k(x,y) = 0$, et que

l'identité de Hall s'écrit :

$$\text{(I)} \quad h(h(x,y),k(z,y)) * h(h(y,z),k(x,z)) * h(h(z,x),k(y,x)) = 0$$

Nous allons montrer que cette relation est impossible si $h(x,y) \neq 0$ et si K est sans éléments nilpotents. Nous ordonnerons lexicographiquement les monomes en x,y,z, posant ainsi $c\, x^i\, y^j\, z^k < c'\, x^{i'}\, y^{j'}\, z^{k'}$ si $c,c' \in K$; $c,c' \neq 0$, et si la première des 3 différences $(i' - i)$, $(j' - j)$, $(k' - k)$ non nulle est positive.

Soit $c_{\alpha,\beta}\, x^\alpha\, y^\beta$ le monome non nul de rang minimum dans le développemeht de $h(x,y) = \sum_{i,j} c_{i,j}\, x^i\, y^j$,en supposant que $h \neq 0$. Puisque $h(0,y) = h(x,0) = 0$, nous avons certainement $\alpha \geqslant 1$.

L'identité (en notation multiplicative) : $(y,x) = (x,y)^{-1}$ conduit à la relatior entre séries formelles : $h(y,x) = g(h(x,y)) = -h(x,y) + \sum_{i=2}^{\infty} b_i\, h(x,y)^i$. Nous en déduisons que $c_{i,j} = 0$ si $j < \alpha$, et que $c_{i,j} + c_{j,i} = 0$ si i (ou j) est égal à α .

Distinguons deux cas.

1°) $\alpha > 1$. Alors tous les monomes du développement de $h(h(x,y),k(z,y))$ (resp. de $h(h(z,x),k(y,x))$) sont de degré au moins égal à $\alpha^2 > \alpha$ par rapport à x . Par contre, le développement de $h(h(y,z),k(x,z))$ contient des monomes non nuls en x^α , et un calcul très facile montre que le monome de rang minimum est :

$$-c_{\alpha,\beta}^{\beta+1}\, x^\alpha\, y^{\alpha\beta}\, z^{\beta^2} \qquad \text{(On a } c_{\alpha,\beta}^{\beta+1} \neq 0 \text{ parce que } c_{\alpha,\beta} = 0$$

et que K est sans éléments nilpotents). L'identité de Hall ne peut pas être vérifiée, car les termes de premier degré en x,y,z dans le développement de $x * y * z$ se réduisent à $x + y + z$. Le développement du premier membre de (I) contiendrait le monome de rang minimum non nul déjà calculé, ce qui est impossible.

2°) $\alpha = 1$. Le raisonnement précédent n'est plus applicable, mais les termes du premier degré en x dans le développement du premier membre de (I) se réduisent à la somme des termes de degré 1 en x dans les trois "facteurs" : $h(h(x,y),k(z,y))$, etc ...

Les termes de degré 1 en x dans le développement de $h(h(x,y),k(z,y))$ se réduisent à $\sum_{i,j} c_{1,i}\, c_{1,j}\, x\, y^i\, k(z,y)^j$.

Les termes de degré 2 en x dans le développement de $h(h(z,x),k(y,x))$ sont tous contenus dans le développement de $\sum_{i,j} c_{j,1}\, c_{1,i}\, x\, k(y,x)^i\, z^j$.

Or $k(y,0) = y$. Les termes cherchés sont donc : $\sum_{i,j} c_{j,1}\, c_{1,i}\, x\, y^i\, z^j$. Si nous tenons compte de la relation $c_{1,j} + c_{j,1} = 0$, nous voyons que la somme des termes de degré 1 en x dans le développement de $h(h(x,y),k(z,y)) + h(h(z,x),k(y,x))$ est donnée par : $\sum_{i,j} c_{1,i}\, c_{1,j}\, x\, y^i\, (k(z,y)^j - z^j)$. Or tous les termes du développement de $k(z,y) - z$ sont de degré au moins égal à 1 en y . Nous voyons donc que tous les termes de degré 1 en x dans $h(h(x,y),k(z,y)) + h(h(z,x),k(y,x))$ sont de degré au moins égal à $(\beta + 1)$ en y .

Par contre, dans le développement de $h(h(y,z),k(x,z))$, nous trouvons le monome non nul de rang minimum :

$$- c_{1,\beta}^{\beta+1}\, x\, y^{\beta}\, z^{\beta^2}$$, qui apparait donc dans le premier membre du développement de (I).

L'hypothèse que $f(x,y)$ n'est pas abélienne conduit donc à une contradiction si K est sans éléments nilpotents, ce qui démontre le théorème.

Ce théorème ne serait plus exact si l'on n'imposait aucune condition à l'anneau de base K . En voici un contre-exemple. K est l'algèbre de dimension 2 sur le corps F_2 à 2 éléments possédant une base formée de l'élément unité et d'un élément a de carré nul ($a^2 = 0$) ; on vérifie alors immédiatement que $x+y+axy^2$ est une loi de groupe non abélienne à coefficients dans K .

Dans les applications, K est le plus souvent un corps ; la restriction imposée par le théorème 1 est donc peu gênante.

Si φ et ψ sont deux séries formelles en x , à coefficients dans K , nous noterons $\varphi \circ \psi$ la série composée : $\varphi \circ \psi\ (x) = \varphi(\psi(x))$.

Nous désignerons par $G(K)$ l'ensemble des séries formelles en x à coefficients dans K telles que, si $\varphi(x) \in G(K)$,

$$\varphi(x) \equiv cx \quad (\text{mod.deg.}2) , \tag{1.4}$$

où c est un élément <u>inversible</u> de K . Si $\varphi(x) \in G(K)$, il existe une série formelle et une seule, notée $\varphi^{-1}(x)$, telle que $\varphi^{-1} \circ \varphi(x) = \varphi \circ \varphi^{-1}(x) = x$. L'ensemble $G(K)$ est ainsi un <u>groupe</u> par rapport à l'opération $\circ$.

Dans $G(K)$ nous considérerons le <u>sous-groupe invariant</u> $G_1(K)$ formé des séries $\varphi(x)$ telles que :

$$\varphi(x) = x \quad (\text{mod.deg.}2). \tag{1.5}$$

Si $f(x)$ (resp. $f(x,y)$) est une série formelle à coefficients dans K , nous appellerons <u>transmutée</u> de f par $\varphi(x) \in G(K)$ la série :

$$(1.6) \qquad f^{\varphi} = \varphi(f(\varphi^{-1}(x))) \qquad \text{,ou, respectivement,}$$

$$(1.7) \qquad f^{\varphi} = \varphi(f(\varphi^{-1}(x),\varphi^{-1}(y))) \ .$$

Si f est une loi de groupe à coefficients dans K , il en est de même de la série transmutée f^{φ} , quel que soit $\varphi \in G(K)$. Il est clair que le groupe $G(K)$ <u>opère</u> sur l'ensemble des lois de groupes, d'après :

$$(1.8) \qquad f^{\varphi \circ \psi} = (f^{\psi})^{\varphi} \quad ;$$

l'ensemble des lois de groupes se partage ainsi en classes de transitivité suivant le groupe $G(K)$ ou son sous-groupe $G_1(K)$. Nous dirons que deux lois f et g sont équivalentes au sens fort (resp.équivalentes au sens faible) si elles sont transmutées l'une en l'autre par un élément de $G(K)$ (resp. de $G_1(K)$).

Si f est une loi de groupe, nous appellerons <u>stabilisateur</u> (resp. stabilisateur faible) de f le sous-groupe de $G(K)$ (resp. de $G_1(K)$) constitué par les éléments φ tels que $f^{\varphi} = f$.

<u>Lemme 1</u>.- Soient $f(x_1,\ldots,x_r)$, $g_i(y_1,\ldots,y_s)$, $g_i'(y_1,\ldots,y_s)$ des séries formelles à coefficients dans le même anneau K $(1 \leqslant i \leqslant r)$. On suppose que :

$$f \equiv 0 \qquad (\text{mod.deg.}q)$$

$$g_i \equiv g_i' \qquad (\text{mod.deg.}q') \text{ , pour } 1 \leqslant i \leqslant r \ .$$

Alors : $f(g_1,\ldots,g_r) \equiv f(g_1',\ldots,g_r') \qquad (\text{mod.deg.}(q+q'-1))$.

<u>Démonstration</u>.- Désignons par $g_{i,j}$ et $g_{i,j}'$ les composantes homogènes de degré j de g_i et g_i' respectivement. Une fois connue la série f , la composante homogène de degré k de $f(g_1,\ldots,g_r)$ se calcule sous la forme d'un polynôme $P((g_{i,j}))$ dont tous les termes ont un degré total $\geqslant q$. Nous obtenons la composante homogène de degré k de $f(g_1',\ldots,g_r')$ sous la même forme $P(g_{i,j}'))$. Si nous substituons les $(g_{i,j}')$ aux $(g_{i,j})$ dans un monome de P qui ne fait pas intervenir effectivement les $g_{i,j}$ où $j \geqslant q'$, nous retrouvons identiquement les mêmes termes. Si, par contre, le monome contient un $g_{i,j}$ où $j \geqslant q'$, son développement ne contient que des termes de degré total $(q+q'-1)$ par rapport aux indéterminées y. Notre lemme est donc démontré.

Ce lemme sera très souvent utilisé dans les calculs que nous serons amenés à effectuer, et dont nous épargnerons au lecteur les détails les plus fastidieux.

2.- La loi de groupe universelle.-

Soit $f(x,y) = \sum_{i,j} a_{i,j}\, x^i\, y^j$ une loi de groupe à coefficients dans l'anneau K, et u un homomorphisme de K dans un autre anneau K'[1]. Considérons alors la série formelle $u.f(x,y) = \sum_{i,j} u(a_{i,j})\, x^i\, y^j$. Une vérification immédiate montre que $u.f(x,y)$ est une loi de groupe à coefficients dans K'. Cette proposition simple nous donne le moyen d'obtenir toutes les lois de groupe abéliennes. Nous démontrerons en effet le :

Théorème 2.- Il existe un anneau A et une loi de groupe abélienne $F(x,y)$ à coefficients dans A tels que toute loi de groupe abélienne à coefficients dans un anneau unitaire quelconque K s'obtienne d'une manière et d'une seule sous la forme $u.F(x,y)$, où u est un homomorphisme de A dans K.[2]

Nous dirons alors que $F(x,y)$ est une loi de groupe universelle. Si $F(x,y)$ et $F'(x,y)$ sont deux lois de groupes universelles à coefficients dans les anneaux A et A' respectivement, le théorème 2 prouve l'existence d'un couple d'isomorphismes réciproques u et u' (de A sur A' et de A' sur A, respectivement), tels que $F' = u.F$ et $F = u'.F'$. Une loi universelle et son anneau des coefficients sont donc déterminés à un isomorphisme canonique près.

Nous démontrerons le théorème 2 en construisant, suivant l'ordre croissant de leur degré total, les composantes homogènes de $F(x,y)$. Introduisons d'abord la notion de bourgeon.

Définition . Nous dirons qu'une série formelle $f(x,y)$ détermine un q-bourgeon (q entier $\geqslant 1$) si les conditions suivantes sont vérifiées :

$$(2.1)\qquad \begin{cases} \text{a)} & f(x,y) \equiv x + y \qquad (\text{mod.deg.}2) \\ \text{b)} & \Gamma f(x,y,z) \equiv 0 \qquad (\text{mod.deg.}(q+1)) \end{cases}$$

Si f et f' sont deux séries telles que $f(x,y) \equiv f'(x,y)$ (mod.deg. $(q+1)$), le lemme 1 montre que $\Gamma f(x,y,z) = \Gamma f'(x,y,z)$ (mod.deg.$(q+1)$).

---

[1] Lorsque nous considérons un homomorphisme d'anneaux unitaires (possédant une unité); nous supposons toujours que l'homomorphisme est unitaire (c'est-à-dire met en correspondance les unités des deux anneaux). Nous avons donc ici : $u(1) = 1$.

[2] Le même théorème est valable pour les lois de groupes abéliennes à un nombre quelconque de paramètres.

Par conséquent, si f détermine un q-bourgeon, il en est de même de f' ; nous conviendrons alors de dire que f et f' déterminent le même q-bourgeon. Un q-bourgeon est donc une classe de séries définies (mod.deg.$(q + 1)$), et vérifiant (2.1) ; si l'on veut considérer un représentant déterminé de cette classe de séries, il suffira de prendre le polynôme dont tous les monomes de degré total $> q$ sont nuls.

Toute série $f(x,y)$ qui détermine un q-bourgeon vérifie (cf.(1.3.c)) :

$$(2.1.c) \qquad f(0,x) \equiv f(x,0) \equiv x \qquad (\text{mod.deg.}(q + 1)) .$$

Les conditions (2.1) sont évidemment plus faibles que les conditions (1.3) : toute loi de groupe détermine, pour tout entier q , un q-bourgeon. Mais il n'est pas toujours vrai qu'un q-bourgeon puisse être déterminé par une loi de groupe. Considérons, par exemple, le cas où l'anneau des coefficients est le corps premier F_2 . Alors $f(x,y) = x + y + xy^2$ détermine un 4-bourgeon qui ne peut être déterminé par aucune loi de groupe, puisque (théorème 1) les lois de groupes sur F_2 sont abéliennes.

Nous dirons qu'un q'-bourgeon <u>prolonge</u> un q-bourgeon si $q' \geqslant q$ et si toute série qui détermine le q'-bourgeon détermine en même temps le q-bourgeon ; autrement dit les deux bourgeons doivent avoir mêmes composantes homogènes de degré total $\leqslant q$. Nous dirons de même qu'une loi de groupe prolonge un q-bourgeon si elle le détermine.

Nous dirons qu'un q-bourgeon est abélien si toute série f qui le détermine vérifie : $f(x,y) \equiv f(y,x)$ (mod.deg.$(q + 1)$). Nous démontrerons la :

<u>Proposition 1</u>.- Tout q-bourgeon abélien est prolongeable en une loi de groupe (quel que soit l'entier positif q et l'anneau des coefficients).

Etudions d'abord le problème du "<u>prolongement élémentaire</u>" : étant donné un q-bourgeon déterminé par une série $f(x,y)$, cherchons un $(q + 1)$ q-bourgeon qui le prolonge.

Désignons généralement par $\Gamma_{q+1} f(x,y,z)$ la composante homogène de degré total $(q + 1)$ de $\Gamma f(x,y,z)$. D'après (2.1.b), nous avons :

$\Gamma f(x,y,z) \equiv \Gamma_{q+1} f(x,y,z)$ (mod.deg.$(q+2)$) . Il faut trouver un polynome $h(x,y)$, homogène de degré $(q + 1)$, tel qu'en posant : $f' = f + h$, on ait :

$\Gamma_{q+1} f'(x,y,z) = 0$.

La série $f'(x,y)$ détermine alors un $(q+1)$-bourgeon qui prolonge le q-bourgeon donné.

<u>Lemme 2</u>.- Avec les motations précédentes, on a :

$$\Gamma_{q+1} f'(x,y,z) = \Gamma_{q+1} f(x,y,z) - \delta h(x,y,z) ,$$

où $$\delta h(x,y,z) = h(y,z) - h(x+y,z) + h(x,y+z) - h(x,y)$$

<u>Démonstration</u>. Posons $g(x,y) = f(x,y) - x - y$. D'après le lemme 1 :

$$f'(f'(x,y),z) = f(f'(x,y),z) + h(f'(x,y),z) \equiv f(f'(x,y),z) + h(x+y,z) \quad (\text{mod.deg.}(q+2)).$$

Ensuite, en appliquant encore le lemme 1 :

$$f(f'(x,y),z) = f'(x,y)+z+g(f'(x,y),z) = f(x,y)+h(x,y)+z+g(f(x,y),z) \quad (\text{mod.deg.}(q+2)).$$

Nous obtenons ainsi :

$$f'(f'(x,y),z) = f(f(x,y),z) + h(x,y) + h(x+y,z) \quad (\text{mod.deg.}(q+2)). \tag{2.2}$$

Nous démontrerions de même :

$$f'(x,f'(y,z)) = f(x,f(y,z) + h(y,z) + h(x,y+z) \quad (\text{mod.deg.}(q+2)). \tag{2.3}$$

Les relations (2.2) et (2.3) entraînent le lemme 2. Nous en désuisont la :

<u>Proposition 2</u>. Le q-bourgeon déterminé par une série $f(x,y)$ est prolongeable en un $(q+1)$-bourgeon si et seulement s'il existe un polynome $h(x,y)$, homogène de degré $(q+1)$, tel que : $\delta h(x,y,z) = \Gamma_{q+1} f(x,y,z)$.

<u>Définitions</u>. Pour tout entier $q \geqslant 2$, nous désignerons par $B_q(x,y)$ le polynome à coefficients entiers :

$$B_q(x,y) = (x+y)^q - x^q - y^q . \tag{2.4}$$

Pour tout entier $q \geqslant 2$, nous désignerons par $C_q(x,y)$ le polynome à coefficients entiers :

$$\left\{ \begin{array}{ll} C_q(x,y) = B_q(x,y) & \text{, si } q \text{ n'est pas une puissance entière d'un nombre premier.} \\ C_q(x,y) = \frac{1}{p} B_q(x,y) & \text{, si } q = p^h \text{, où } p \text{ est un nombre premier et } h \text{ un entier naturel.} \end{array} \right. \tag{2.5}$$

Le fait que les polynomes C_q soient à coefficients entiers résulte de la relation bien connue : $(x+y)^p \equiv x^p + y^p \pmod{p}$, où p est un nombre premier.

<u>Lemme 3</u>. Soit K un anneau quelconque. Pour tout entier $q \geqslant 2$, les seuls polynomes $P(x,y) \in K[x,y]$ qui soient homogènes de degré q et qui vérifient :

$$(2.6) \qquad \begin{cases} \text{a)} \quad \delta P(x,y,z) = P(y,z) - P(x+y,z) + P(x,y+z) - P(x,y) = 0 \\ \text{b)} \quad P(x,y) - P(y,x) = 0 \end{cases}$$

sont de la forme $aC_q(x,y)$, où $a \in K$.

Pour ne pas interrompre notre exposé, la démonstration de ce lemme sera donnée au paragraphe 3. Nous admettrons aussi provisoirement le résultat suivant : pour tout $q \geqslant 2$, les coefficients de $C_q(x,y)$ sont des entiers premiers entre eux dans leur ensemble.

Des lemmes 2 et 3 nous déduisons immédiatement la :

<u>Proposition 3</u>. Soient $f(x,y)$ et $g(x,y)$ deux séries formelles à coefficients dans K, telles que $f \equiv g \pmod{\deg.q}$, et que f et g déterminent toutes deux des q-bourgeons abéliens. Alors il existe $a \in K$ tel que :

$$f(x,y) = g(x,y) + aC_q(x,y) \qquad (\text{mod.deg.}(q+1)).$$

Introduisons maintenant une famille dénombrable d'indéterminées (α_i), $i = 1,2,\ldots$ et désignons par :

$A = Z[(\alpha_i)]$	l'anneau des polynomes à coefficients entiers par rapport à tous les (α_i).
$A_q = Z[\alpha_1,\ldots,\alpha_q]$	l'anneau des polynomes à coefficients entiers par rapport à $(\alpha_1,\ldots,\alpha_q)$.
$A' = Q[(\alpha_i)]$	l'anneau des polynomes à coefficients rationnels par rapport à tous les (α_i).
$A'_q = Q[\alpha_1,\ldots,\alpha_q]$	l'anneau des polynomes à coefficients rationnels par rapport à $(\alpha_1,\ldots,\alpha_q)$.

Des identifications évidentes nous permettent d'écrire les inclusions :

$$(2.7) \begin{cases} A_1 \subset A_2 \subset \ldots A_q \subset A_{q+1} \subset \ldots \subset A \ ; \ A'_1 \subset A'_2 \subset \ldots A'_q \subset A'_{q+1} \subset \ldots \subset A' \\ A_q \subset A'_q \quad , \text{ pour tout entier } q \text{ et } A \subset A' . \end{cases}$$

Nous considérerons de même $A_q[[x,y]]$ comme un sous-anneau de $A'_q[[x,y]]$, etc...

<u>Proposition 4</u>. Il existe deux suites de séries formelles $f_q(x,y)$ et $\varphi_q(x)$, telles que, pour tout entier $q \geqslant 1$, on ait :

$$(2.8)\quad \begin{array}{ll} \text{a)} & f_q(x,y) \in A_q\,[[x,y]] \quad \text{et} \quad \varphi_q(x) \in G_1(A'_q) \;; \\ \text{b)} & f_q \equiv f_{q+1} \quad \text{et} \quad \varphi_q \equiv \varphi_{q+1} \quad (\text{mod.deg.}(q+2)) \;; \\ \text{c)} & f_q(x,y) - \alpha_q C_{q+1}(x,y) \in A_{q-1}\,[[x,y]] \;; \\ \text{d)} & f_q^{\varphi_q}(x,y) \equiv x + y \quad (\text{mod.deg.}(q+2)) \;. \end{array}$$

<u>Démonstration</u>. Nous allons construire successivement les couples de séries f_q, φ_q. Nous prendrons d'abord :

$$(2.9)\qquad f_1(x,y) = x+y+\alpha_1 xy \quad \text{et} \quad \varphi_1(x) = x - \tfrac{1}{2}\alpha_1 x^2 \;.$$

On vérifie immédiatement que les conditions (2.8) sont satisfaites en ce qui concerne f_1 et φ_1. Nous supposerons déjà construits $f_1,\ldots,f_q$; $\varphi_1,\ldots,\varphi_q$ vérifiant (2.8). Nous pourrons supposer de plus que chaque f_r déjà construit est un polynome (non homogène) de degré total (r+1), car on peut remplacer chaque f_r par n'importe quelle série à coefficients dans A_r qui lui est congrue (mod. deg.(r+2)) sans cesser de vérifier les conditions (2.8). Cherchons donc à déterminer f_{q+1} et φ_{q+1}.

Les relations (2.8.a) et (2.8.d) montrent que f_q détermine un (q+1)-bourgeon à coefficients dans A_q. Désignons, conformément aux notations précédentes, par $\Gamma_{q+2} f_q(x,y,z)$ la composante homogène de degré (q+2) de $\Gamma f_q(x,y,z)$; c'est, d'après (2.8.a), un polynome à coefficients dans A_q. Posons :

$$(2.10)\qquad g_q(x,y) = \varphi_q^{-1}\,(\varphi_q(x) + \varphi_q(y)).$$

La série $g_q(x,y)$ est, d'après (2.8.a), une loi de groupe à coefficients dans A'_q. De plus, la relation (2.8.d) implique :

$$(2.11)\qquad f_q = (f_q^{\varphi_q})^{\varphi_q^{-1}} \equiv g_q \quad (\text{mod.deg.}(q+2)).$$

Soit $h(x,y)$ la composante homogène de degré (q+2) de $g_q(x,y)$, de telle sorte que :

$$(2.12)\qquad g_q(x,y) \equiv f_q(x,y) + h(x,y) \quad (\text{mod.deg.}(q+3)).$$

D'après le lemme 2, nous avons :

(2.13) $$\delta h(x,y,z) = \Gamma_{q+2} f_q(x,y,z) \in A_q[x,y,z],$$

et, puisque g_q est une loi abélienne :

(2.14) $$h(x,y) - h(y,x) = 0 .$$

Le polynome h appartient à $A'_q[x,y]$; puisque tout élément de A'_q possède un multiple entier dans A_q, il existe un entier naturel n tel que :

(2.15) $$nh(x,y) \in A_q[x,y] .$$

Désignons par $\hat{A}_q$ l'anneau A_q réduit modulo n, c'est-à-dire l'anneau quotient A_q/nA_q, et notons $\hat{k}(x,y)$ le polynome obtenu à partir de $nh(x,y)$ en remplaçant chaque coefficient par son image canonique dans $\hat{A}_q$. Les relations (2.13) et (2.14) nous donnent :

(2.16) $$\begin{cases} \delta\hat{k}(x,y,z) = 0 \\ \hat{k}(x,y) - \hat{k}(y,x) = 0 \end{cases}$$

Par conséquent, d'après le lemme 3 :

(2.17) $$\hat{k}(x,y) = \hat{a}C_{q+2}(x,y) \quad , \text{ où } \hat{a} \in \hat{A}_q .$$

Soit $a \in A_q$ un élément dont l'image canonique dans $\hat{A}_q$ soit $\hat{a}$. La relation (2.17) s'écrit encore (en remplaçant les égalités dans $\hat{A}_q$ par des congruences (mod.n) dans A_q) :

(2.18) $$nh(x,y) = aC_{q+2}(x,y) + nh'(x,y) \quad , \text{ où } h'(x,y) \in A_q[x,y].$$

Définissons alors f_{q+1} et φ_{q+1} par les relations :

(2.19) $$f_{q+1}(x,y) = f_q(x,y) + h'(x,y) + \alpha_{q+1}C_{q+2}(x,y) .$$

(2.20) $$\begin{cases} \varphi_{q+1}(x) = \varphi_q(x) + (\frac{a}{n} - \alpha_{q+1})x^{q+2} & \text{si } (q+2) \text{ n'est pas une puissance d'un nombre premier ;} \\ \varphi_{q+1}(x) = \varphi_q(x) + \frac{1}{p}(\frac{a}{n} - \alpha_{q+1})x^{q+2} & \text{si } (q+2) \text{ est une puissance du nombre premier } p. \end{cases}$$

Les conditions (2.8.a,b,c) sont évidemment satisfaites. Pour vérifier (2.8.d) nous nous appuierons sur le lemme suivant.

<u>Lemme 4</u>. Soient $f(x,y)$ une série formelle à coefficients dans l'anneau K telle que $f(x,y) \equiv x + y$ (mod.deg.2), et $g(x,y)$ une série formelle telle que $g(x,y) \equiv f(x,y) + k(x,y)$ (mod.deg.(q+1)) , où $k(x,y)$ est un polynome homogène de degré q (entier $\geqslant 2$) . Soient $\varphi(x)$ et $\psi(x)$ deux éléments de $G_1(K)$ tels que $\psi(x) \equiv \varphi(x)+bx^q$ (mod.deg.(q+1)), où $b \in K$. Alors :

$$g^{\psi}(x,y) = f^{\varphi}(x,y) + k(x,y) + bB_q(x,y) \quad \text{(mod.deg.(q+1))}.$$

<u>Démonstration</u>. Nous utiliserons le lemme 1 pour démontrer successivement :

$$\psi^{-1}(x) \equiv \varphi^{-1}(x) - bx^q \quad \text{(mod.deg.(q+1))}. \tag{2.21}$$

$$g(\psi^{-1}(x),\psi^{-1}(y)) \equiv g(\varphi^{-1}(x),\ \varphi^{-1}(y))-b(x^q+y^q) \quad \text{(mod.deg.(q+1))} \tag{2.22}$$

$$g(\varphi^{-1}(x),\varphi^{-1}(y)) \equiv f(\varphi^{-1}(x),\ \varphi^{-1}(y))+k(x,y) \quad \text{(mod.deg.(q+1))}. \tag{2.23}$$

$$\psi(f(\varphi^{-1}(x),\varphi^{-1}(y))+k(x,y)-b(x^q+y^q)) = f^{\varphi}(x,y)+k(x,y)+bB_q(x,y) \quad \text{(mod.deg.(q+1))} \tag{2.24}$$

Les trois dernières congruences entraînent le lemme 4.

Achevons la démonstration de la proposition 4. D'après (2.12),(2.18) et (2.19) nous avons :

$$f_{q+1}(x,y) \equiv g_q(x,y)+(\alpha_{q+1}-\tfrac{a}{n})C_{q+2}(x,y) \quad \text{(mod.deg.(q+3))} \tag{2.25}$$

Appliquons maintenant le lemme 4 (où nous remplaçons respectivement K,q,f,φ,ψ par A'_{q+1} , $(q+2),g_q,f_{q+1}$, φ_q, φ_{q+1}) ; nous obtenons :

$$f_{q+1}^{\varphi_{q+1}}(x,y) \equiv g_q^{\varphi_q}(x,y) = x + y \quad \text{(mod.deg.(q+3))}, \tag{2.26}$$

ce qui établit (2.8.d) pour l'indice (q+1).

Nous supposons donc construites les séries $f_q(x,y)$ et $\varphi_q(x)$ vérifiant les conditions de la proposition 4. Définissons les séries $F(x,y) \in A[[x,y]]$ et $\varphi(x) \in A'[[x]]$ par les conditions :

$$\begin{cases} F(x,y) \equiv f_q(x,y) & \text{(mod.deg.(q+2))} \text{ , pour tout } q \quad 1 \text{ ;} \\ \varphi(x) \equiv \varphi_q(x) & \text{(mod.deg.(q+2))}, \text{ pour tout } q \quad 1 \text{ .} \end{cases} \tag{2.27}$$

Ces conditions sont compatibles (2.8.b), et nous avons, d'après (2.8.d) :

$$(2.28) \qquad F^{\varphi}(x,y) = x + y \ .$$

La série F est donc une loi de groupe abélienne à coefficients dans A. Nous sommes maintenant en mesure de démontrer la proposition 1 en même temps que le théorème 2.

Soit K un anneau unitaire et $g(x,y)$ une série à coefficients dans K qui détermine un q-bourgeon abélien. Remarquons que l'anneau A_r est l'<u>anneau unitaire libre</u> engendré par $(\alpha_1,\ldots,\alpha_r)$ et que, par conséquent, un homomorphisme u_r de A_r dans K est entièrement déterminé par la donnée de $u_r(\alpha_1),\ldots,u_r(\alpha_r)$ qui peuvent être choisis arbitrairement dans K.

Supposons déterminé pour un entier $r(1 \leq r \leq q-1)$ un homomorphisme u_r de A_r dans K tel que [1] :

$$(2.29) \qquad u_r.f_r(x,y) \equiv g(x,y) \qquad (\text{mod.deg.}(r+2)).$$

Pour $r=1$, l'homomorphisme u_1 existe et est unique, puisque $f_1(x,y) = x+y+\alpha_1 xy$. Définissons l'homomorphisme u'_r de A_{r+1} dans K en convenant que $u'_r(\alpha_{r+1}) = 0$ et que u'_r coïncide avec u_r sur A_r. Alors :

$$(2.30) \qquad u'_r.f_{r+1}(x,y) \equiv g(x,y) \qquad (\text{mod.deg.}(r+2)).$$

Si $q \geqslant (r+2)$, les séries $u'_r.f_{r+1}(x,y)$ et $g(x,y)$ déterminent toutes deux des $(r+2)$-bourgeons abéliens, et, d'après la proposition 3, il existe un élément $c_r \in K$ tel que :

$$(2.31) \qquad g(x,y) \equiv u'_r.f_{r+1}(x,y) + c_r C_{r+2}(x,y) \qquad (\text{mod.deg.}(r+3)).$$

Pour qu'un homomorphisme u_{r+1} de A_{r+1} dans K prolonge u_r et vérifie (2.29) où l'on remplace r par $(r+1)$, il faut et il suffit que $u_{r+1}(\alpha_{r+1}) = c_r$. Cette condition est en effet suffisante, d'après (2.8.c). Elle est nécessaire, car, d'après (2.31), on doit avoir : $u_{r+1}(\alpha_{r+1})C_{r+2}(x,y) = c_r C_{r+2}(x,y)$; or nous avons admis que les coefficients de $C_{r+2}(x,y)$ sont premiers entre eux dans leur ensemble. Les éléments $u_{r+1}(\alpha_{r+1})$ et c_r s'obtiennent donc comme une combinaison

---

[1] Nous généralisons ici la notation $u.f(x,y)$ introduite au début de ce paragraphe à des séries qui ne sont plus des lois de groupes. Il s'agit toujours d'appliquer l'homomorphisme u aux coefficients de la série considérée.

linéaire à coefficients entiers des mêmes éléments de K, ce qui établit que $u_{r+1}(\alpha_{r+1}) = c_r$.

Partant de l'homomorphisme u_1, et poursuivant notre construction jusqu'à u_{q-1}, nous voyons qu'il existe un homomorphisme u_{q-1} de A_{q-1} dans K, uniquement déterminé par la condition (2.29), où l'on remplace r par $(q-1)$. Soit u un homomorphisme de A dans K qui prolonge u_{q-1}. Alors la série $u.F(x,y)$ est une loi de groupe à coefficients dans K qui prolonge le q-bourgeon déterminé par $g(x,y)$: la proposition 1 est démontrée.

Supposons maintenant que $g(x,y)$ soit une loi de groupe abélienne à coefficients dans K. Alors les homomorphismes u_r sont univoquement déterminés par la condition (2.29), pour tout $r \geqslant 1$. Il existe un homomorphisme unique u de A dans K qui prolonge tous les homomorphismes u_r, et l'on a : $u.F(x,y) = g(x,y)$, ce qui démontre le théorème 2.

L'anneau A' peut être caractérisé comme le produit tensoriel de l'anneau A par le corps Q des nombres rationnels. Si l'anneau K est une algèbre sur le corps Q, tout homomorphisme de A dans K se prolonge univoquement en un homomorphisme de A' dans K. Le théorème 2 et la relation (2.28) entraînent donc la :

<u>Proposition 5</u>. Toute loi de groupe abélienne $f(x,y)$ dont l'anneau des coefficients est une algèbre sur le corps des nombres rationnels est équivalente (au sens faible) à la loi $x+y$.

Nous démontrerons plus loin (3.14.a) que toute loi de groupe à coefficients dans une Q-algèbre est abélienne.

(2.32) <u>Remarques</u>. a) Les conditions (2.8) de la proposition 4 ne suffisent pas à déterminer univoquement les séries $f_q(x,y)$. A moins d'imposer des conditions faciles à imaginer, mais absolument artificielles, je ne vois pas comment "choisir" parmi les lois universelles possibles. La notion naturelle d'unicité pour la loi universelle $F(x,y)$ est exposée dans la remarque qui suit immédiatement l'énoncé du théorème 2.

b) Considérons les polynomes $f(x,y) =$

$= x + y + \sum_{2 \leqslant i+j \leqslant q} a_{i,j} x^i y^j$ qui déterminent des q-bourgeons abéliens. Leurs coefficients $a_{i,j}$ doivent annuler un certain nombre de polynomes à coefficients entiers. Ils constituent donc une variété algébrique dont il est inutile de préciser le corps (ou même l'anneau !) de définition. Cette variété algébrique est un espace affine de dimension (q-1), c'est-à-dire qu'on peut trouver des "para-

mètres" $\alpha_1,\ldots,\alpha_{q-1}$ qui s'expriment comme des combinaisons linéaires à coefficients entiers des $a_{i,j}$, et tels que les $a_{i,j}$ s'expriment comme des polynomes à coefficients entiers par rapport aux $\alpha_1,\ldots,\alpha_{q-1}$. Cette remarquable simplicité de structure est assez cachée : le lecteur qui voudra tenter les calculs verra qu'il n'est pas aisé de déterminer les coefficients d'une loi universelle, même en se bornant aux termes de degré petit ($\leqslant 10$, par exemple). Il serait donc souhaitable de trouver une détermination plus explicite d'une loi de groupe universelle $F(x,y)$.

3.- <u>Démonstration du lemme 3</u>.-

Démontrons d'abord que, si q n'est pas une puissance du nombre premier p :

(3.1) $$B_q(x,y) \not\equiv 0 \pmod{p}.$$

Posons en effet $q = p^h s$, où $s \neq 1$, $s \not\equiv 0 \pmod{p}$. Alors :

$$(x+y)^q \equiv (x^{p^h} + y^{p^h})^s = x^q + sx^{(s-1)p^h}y^{p^h} + \ldots + y^q \pmod{p}$$ et par conséquent :

(3.2) $$B_q(x,y) = sx^{(s-1)p^h}y^{p^h} + \ldots \not\equiv 0 \pmod{p}.$$

Si maintenant $q = p^h$, nous avons :

$$(x+y)^{p^{h-1}} \equiv x^{p^{h-1}} + y^{p^{h-1}} \pmod{p},$$ d'où (1)

$$(x+y)^{p^h} \equiv (x^{p^{h-1}} + y^{p^{h-1}})^p \pmod{p^2}.$$ Il en résulte :

(3.3) $$C_{p^h}(x,y) \equiv C_p(x^{p^{h-1}}, y^{p^{h-1}}) \not\equiv 0 \pmod{p}.$$

Les relations (3.1) et (3.3) montrent que, quel que soit l'entier $q \geqslant 2$, <u>les coefficients du polynome</u> $C_q(x,y)$ <u>sont premiers entre eux dans leur ensemble</u>.

Considérons maintenant un anneau quelconque K, et proposons nous d'étudier les polynomes $P(x,y) = \sum_{i=0}^{q} a_{i,q-i}\, x^i y^{q-i}$, où $a_{i,q-i} \in K$, tels que :

(3.4) $$\delta P(x,y,z) = P(y,z) - P(x+y,z) + P(x,y+z) - P(x,y) = 0.$$

Nous avons d'abord $\delta P(x,0,0) = P(0,0) - P(x,0) = 0$ et $\delta P(0,0,z) = P(0,z) - P(0,0) = 0$, relations équivalentes à :

(3.5) $$a_{q,0} = a_{0,q} = 0.$$

(1) - Nous utilisons ici un résultat classique : en élevant à la puissance p les deux membres d'une congruence (mod. p), on obtient une congruence (mod. p^2).

Nous achèverons de traduire l'hypothèse $\delta P = 0$ en écrivant que le coefficient de $x^i y^j z^k$ dans $\delta P(x,y,z)$ est nul, ce qui conduit aux relations :

(3.6) $$\binom{i+j}{j} a_{i+j,k} = \binom{j+k}{j} a_{i,j+k} \quad , \text{ pour } i+j+k = q \quad ; 1 \leqslant i,k \leqslant q-1.$$

En particulier, si nous faisons dans (3.6) $i=1$, puis $j=1$, nous obtenons :

(3.7) $$i a_{i,q-i} = \binom{q-1}{i-1} a_{1,q-1} \quad \text{pour} \quad 1 \leqslant i \leqslant q-1 .$$

(3.8) $$(i+1) a_{i+1,q-i-1} = (q-i) a_{i,q-i} \quad \text{pour} \quad 1 \leqslant i \leqslant q-2 .$$

Prenons d'abord pour anneau de base le <u>corps premier</u> F_p à p éléments.

1°) Supposons $q=p$. Alors, si nous considérons le polynome $P'(x,y) = P(x,y) - a_{1,p-1} C_p(x,y)$, nous avons $\delta P'(x,y,z) = 0$ et donc $P' = 0$, puisque le coefficient de xy^{p-1} dans P' est nul (appliquer (3.7)). Le polynome P est donc un multiple de $C_p(x,y)$.

2°) Supposons $q \equiv 0 \pmod{p}$ et $q \neq p$. Si nous faisons successivement dans (3.8) $i = (p-1),(p-2),\ldots,1$, nous obtenons :

$$a_{p-1,q-p+1} = a_{p-2,q-p+2} = \ldots = a_{1,q-1} = 0 .$$

La relation (3.7) montre alors que : $a_{i,q-i} = 0$ si $i \not\equiv 0 \pmod{p}$. Le polynome $P(x,y)$ peut donc s'écrire sous la forme $P'(x^p,y^p)$, où P' est un polynome de degré q/p à coefficients dans F_p. Mais l'identité $(x+y)^p = x^p + y^p \pmod{p}$ montre que :

(3.9) $$\delta P(x,y,z) = \delta P'(x^p,y^p,z^p) = 0 .$$

Nous sommes ainsi ramenés au degré $q' = q/p$. Si q' est encore divisible par p sans lui être égal, la réduction se poursuit, et nous aboutissons finalement aux résultats suivants : si $q = p^h$, les seuls polynomes P de degré q vérifiant $\delta P = 0$ sont de la forme $aC_{p^h}(x,y)$, où $a \in F_p$; si $q = p^h s$, où $s \neq 1$, $s \not\equiv 0 \pmod{p}$, les polynomes P de degré q vérifiant $\delta P = 0$ sont de la forme $P'(x^{p^h}, y^{p^h})$ où $P'(x,y)$ est un polynome de degré s vérifiant $\delta P' = 0$.

3°) Examinons enfin le cas où $q \not\equiv 0 \pmod{p}$. Puisque le coefficient de xy^{q-1} dans $C_q(x,y)$ n'est pas nul (mod.p), d'après (3.2), nous pouvons prendre

$a \in F_p$, tel que $P'(x,y) = P(x,y) - aC_q(x,y)$ ait son terme en xy^{q-1} nul. Désignons encore par $a_{i,q-i}$ les coefficients du polynome P' . La relation (3.7) montre comme précédemment que $a_{i,q-i} = 0$ si $i \not\equiv 0$ (mod.p). La relation (3.8), où nous faisons $i = rp$ montre que : $a_{rp,q-rp} = 0$, si $rp \leqslant q-2$. Tous les coefficients de P' sont donc nuls, sauf éventuellement celui de $x^{q-1}y$. Nous avons $P'(x,y) = bx^{q-1}y$, avec $b \in F_p$. La condition $\delta P' = 0$ implique alors $b = 0$, sauf si $(q-1)$ est une puissance de p , qui doit être au moins égale à p puisque nous avons supposé que le coefficient de xy^{q-1} dans P' est nul. Si nous tenons compte des résultats obtenus au 2°), nous pouvons résumer ainsi notre étude du cas où l'anneau de base est le corps F_p :

(3.10) Un polynome $P(x,y)$ à coefficients dans F_p, de degré $q \geqslant 2$, et vérifiant $\delta P(x,y,z) = 0$ est de la forme $aC_q(x,y)$, sauf si $q = p^h + p^k$, avec $0 \leqslant h < k$. Dans ce dernier cas, il est de la forme $aC_q(x,y)+bx^{p^k}y^{p^h}$ $(a,b \in F_p)$.

Achevons la démonstration du lemme 3. Considérons, pour un entier $q \geqslant 2$, le module L des polynomes à deux indéterminées x,y , de degré q et à coefficients entiers rationnels. Puisque les coefficients de $C_q(x,y)$ sont premiers entre eux dans leur ensemble, le sous-module $\{C_q\}$ de L formé des multiples entiers de $C_q(x,y)$ est facteur direct dans L, et nous pouvons écrire la somme directe :

$$(3.11) \qquad L = \{C_q\} + M .$$

L'opérateur δ applique L dans le module L' des polynomes à trois indéterminées x,y,z, de degré q et à coefficients entiers ; cet opérateur annule C_q . Soit M' le plus petit sous-module de L' qui contienne δM et soit facteur direct de L' (autrement dit : L'/M' est sans torsion, $\delta M \subset M'$ et $M'/\delta M$ est un groupe fini). Alors le théorème fondamental sur les groupes abéliens de type fini nous apprend qu'on peut choisir des <u>bases</u> $E_i(x,y)$ et $F_i(x,y)$ dans M et M' respectivement $(1 \leqslant i \leqslant q)$, telles que :

$$(3.12) \qquad E_i(x,y,z) = \lambda_i F_i(x,y,z) \quad ,$$

où les λ_i sont des entiers $\geqslant 0$, tels que chaque λ_i soit divisible par λ_{i+1} (pour $1 \leqslant i \leqslant q-1$).

Soit K un anneau quleconque ; le module des polynomes en x et y , à coefficients dans K et de degré q s'obtient sous la forme : $K \otimes L$. Si $P(x,y)$ est un tel polynome, nous pouvons l'écrire sous la forme : $P(x,y) = aC_q(x,y) + \sum_{i=1}^{q} b_i E_i(x,y)$, avec $a,b_i \in K$. La relation $\delta P = 0$ équivaut, d'après

(3.12), à :

(3.13) $\lambda_i b_i = 0$, pour $1 \leq i \leq q$.

Traduisons maintenant le résultat (3.10), en faisant $K = F_p$; nous voyons que $\lambda_i = 1$ pour $2 \leq i \leq q$; $\lambda_1 \neq 0$, et, plus précisément, $\lambda_1 = 1$ sauf si q est somme de deux puissances entières distinctes d'un même nombre premier.

Supposons que $P(x,y) \in K[x,y]$ soit de degré q et vérifie : $\delta P = 0$, $P(x,y) - P(y,x) = 0$. D'après (3.13), $P(x,y) = aC_q(x,y) + bE_1(x,y)$, avec $a,b \in K$ et $\lambda_1 b = 0$. Le polynome $P'(x,y) = \mu P(x,y)$ vérifie les mêmes conditions que P, quel que soit l'entier μ . Supposons $b \neq 0$; nous pouvons choisir μ tel que $\mu b \neq 0$, et que $p\mu b = 0$, p désignant un diviseur premier convenable de λ_1 . Mais, d'après (3.10), on a : $E_1(x,y) \equiv \nu C_q(x,y) + \nu' x^{p^k} y^{p^h}$ (mod.p) , avec $h < k$, et ν, ν' entiers, $\nu \not\equiv 0$ (mod.p).

Alors $P'(x,y) = (a + \mu\nu b)C_q(x,y) + \mu\nu' b x^{p^k} y^{p^h}$. Comme $\mu\nu' b \neq 0$, on voit que P' n'est pas symétrique en x et y . Il est donc absurde de supposer $b \neq 0$, et le lemme 3 est démontré.

(3.14) <u>Remarques</u>. a) Si K, considéré comme groupe abélien, est sans torsion, la seule relation $P = 0$ implique l'existence de $a \in K$ tel que $P = aC_q$. Ce résultat, joint au lemme 2, montre que toute loi de groupe à coefficients dans K est alors abélienne.

b) Un calcul plus poussé montre que λ_1 est égal au produit $p_1 \dots p_r$, où $p_1, \dots, p_r$ sont les nombres premiers tels que q soit somme de deux puissances entières distinctes de chacun d'eux. Par exemple, pour $q = 10$, $\lambda_1 = 6$; pour $q = 30$, $\lambda_1 = 15$.

4.- <u>La classification des lois de groupes</u>.

Le problème à étudier est le suivant : étant donné deux lois de groupes abéliennes f et g à coefficients dans le même anneau K , existe-t-il une série $\varphi(x) \in G(K)$ telle que $f^{\varphi} = g$?

Nous examinerons d'abord un problème de prolongement élémentaire, analogue à celui déjà traité, pour les bourgeons. Soit $\varphi(x) \in G_1(K)$, tel que $f^{\varphi} \equiv g$ (mod.deg.q) ; existe-t-il $\varphi'(x) \in G_1(K)$ tel que $\varphi \equiv \varphi'$ (mod.deg.q), et que $f^{\varphi'} \equiv g$ (mod.deg.(q+1)) ?

D'après la proposition 3, il existe $a \in K$ tel que

$g(x,y) \equiv f(x,y)+aC_q(x,y)$ (mod.deg.(q+1)) . Si $\varphi'(x) = \varphi(x)+bx^q$ (mod.deg.(q+1)), nous avons, d'après le lemme 4 , $f^{\varphi'}(x,y) \equiv f^{\varphi}(x,y)+bB_q(x,y)$ (mod.deg.(q+1)).

Deux cas sont à distinguer. Premier cas : q n'est pas une puissance d'un nombre premier ; alors $B_q = C_q$, il faut prendre $b = a$, et φ' est déterminé (mod.deg.(q+1)). Deuxième cas : $q = p^h$, p premier, h entier > 0 ; alors $B_q = pC_q$; le problème du prolongement élémentaire n'est résoluble que s'il existe $a' \in K$ avec $a = pa'$; il n'est pas nécessairement déterminé, car il faut seulement prendre : $b = a' + b'$, où $b' \in K$, $pb' = 0$.

A partir de ces résultats, on déterminerait sans peine les classes d'équivalence des lois de groupe à coefficients entiers rationnels. Reprenons les notations du théorème 2 et de la proposition 4 ; les lois de groupes $u_i.F(x,y)$ constituent un système complet de représentants de ces classes d'équivalence lorsque u_i parcourt l'ensemble des homomorphismes de A dans Z (anneau des entiers) vérifiant : $u_i(\alpha_q) = 0$ si (q+1) n'est pas puissance d'un nombre premier ; $0 \leq u_i(\alpha_q) < p$ si $(q+1) = p^h$, où p est un nombre premier. On remarquera que $G_1(Z)$ est un sous-groupe d'indice 2 de G(Z), et que si deux lois de groupes à coefficients dans Z sont équivalentes au sens fort, elles sont aussi équivalentes au sens faible (cf., plus loin, (4.4) et (4.5) où l'on fera $n = -1$). L'ensemble des classes d'équivalence des lois de groupes à coefficients dans Z a ainsi la puissance du continu.

Nous nous bornerons désormais à étudier le problème de classification dans le cas où l'anneau de base K est un anneau de caractéristique p (c'est à dire vérifie $pa = 0$ pour tout $a \in K$), p désignant un <u>nombre premier choisi une fois pour toutes</u>. Si p' est un nombre premier distinct de p , il existe, pour tout $a \in K$, un élément a' de K et un seul tel que $p'a' = a$. Cette remarque nous permet d'énoncer plus simplement les résultats concernant le prolongement élémentaire des transmutations :

<u>Proposition 6</u>. Soient f et g deux lois de groupe abélienne à coefficients dans l'anneau K de caractéristique p, et $\varphi(x) \in G_1(K)$ tel que $f^{\varphi} \equiv g$ (mod. deg.q), q entier ≥ 2 . Si q n'est pas une puissance de p, il existe un élément a de K et un seul tel qu'en posant $\varphi'(x) = \varphi(x) + ax^q$, on ait $f^{\varphi'} \equiv g$ (mod.deg.(q+1)). Si $q = p^h$, la relation précédente $f^{\varphi'} \equiv g$ (mod.deg.(q+1)) n'est vérifiée pour aucune valeur de a si $f^{\varphi} \not\equiv g$ (mod.deg.(q+1)), et est vérifiée pour n'importe quelle valeur de $a \in K$ si $f^{\varphi} \equiv g$ (mod.deg.(q+1)).

Ainsi le calcul successif des coefficients $a_1,\dots,a_q,\dots$ de $\varphi(x) = x + \sum_{i=2}^{\infty} a_i x^i$ conduit à des problèmes impossibles ou indéterminés pour $a_p, a_{p^2},\dots,a_{p^h},\dots$ Nous allons étudier comment la possibilité de trouver le coefficient a_{p^h} dépend des <u>choix</u> effectués antérieurement pour $a_p,\dots,a_{p^{h-1}}$.

<u>Définition</u>. Soit $f(x,y)$ une loi de groupe à coefficients dans l'anneau K . Nous appellerons <u>itérés</u> de la loi f la suite des séries $g_n(x)$, définies pour tout entier $n \in Z$, et vérifiant les relations : $g_0(x) = 0$, $g_{n+1}(x) = f(x,g_n(x))$.

Les relations suivantes sont de simples traductions, en termes de séries formelles, de propriétés élémentaires des groupes :

(4.1) $$f(g_n(x),g_{n'}(x)) = g_{n+n'}(x) \quad , \text{ pour tous } n,n' \in Z.$$

(4.2) $$g_n(g_{n'}(x)) = g_{nn'}(x) \quad , \text{ pour tous } n,n' \in Z.$$

Si $\varphi(x) \in G(K)$, et si $g'(x)$ est le n-ième itéré de la loi de groupe $f'(x,y) = f^{\varphi}(x,y)$,

(4.3) $$g'_n(x) = g_n^{\varphi}(x).$$

Si $f(x,y)$ est une loi de groupe <u>abélienne</u>, $g_n(x)$ son n-ième itéré, nous avons :

(4.4) $$g_n(f(x,y)) = f(g_n(x),g_n(y)) \quad , \text{ pour tout } n \in Z.$$

La relation $f(x,y) \equiv x + y \quad (\text{mod.deg.}2)$ entraîne :

(4.5) $$g_n(x) \equiv nx \quad (\text{mod.deg.}2) \quad , \text{ pour tout } n \in Z.$$

Supposons maintenant que $f(x,y)$ soit une loi de groupe abélienne à coefficients dans l'anneau K de caractéristique p. Si son p-ième itéré $g_p(x)$ n'est pas nul, soit q le plus grand entier tel que $g_p(x) \equiv 0 \quad (\text{mod.deg.}q)$. D'après (4.5), $q \geqslant 2$. Soit $\lambda \in K$ tel que $g(x) \equiv \lambda\, x^{q^p} \quad (\text{mod.deg.}(q+1))$. Nous avons : $g_p(f(x,y)) \equiv \lambda\,(x+y)^q \quad (\text{mod.deg.}(q+1))$, et $f(g_p(x),\, g_p(y)) \equiv \lambda\,(x^q+y^q)$ (mod. deg.(q+1)). D'après (4.4), nous en déduisons :

(4.6) $$\lambda\, B_q(x,y) = 0.$$

Puisque $\lambda \neq 0$, cela n'est possible que si q est une puissance de p , d'après (3.2). Ce résultat justifie la définition suivante.

Soit $f(x,y)$ une loi de groupe abélienne à coefficients dans l'anneau K de caractéristique p, et $g_p(x)$ son p-ième itéré. Si $g_p(x) = 0$, nous dirons que f est de <u>hauteur infinie</u>. Sinon nous appellerons <u>hauteur</u> de f le plus grand entier h tel que $g_p(x) \equiv 0 \pmod{\deg.p^h}$.

<u>Lemme 5</u>. Si $f(x,y)$ est une loi abélienne de hauteur h à coefficients dans l'anneau K de caractéristique p, son p-ième itéré $g_p(x)$ est une série $g(x^{p^h})$ en x^{p^h}.

<u>Démonstration</u>. Soit $g_p(x) = \sum_{i=0}^{\infty} \lambda_i x^{p^h+i}$. Démontrons, par récurrence sur i, que $\lambda_i = 0$ si $i \not\equiv 0 \pmod{p^h}$. Supposons démontré que $\lambda_j = 0$ pour $j < i$ et $j \not\equiv 0 \pmod{p^h}$. Nous obtenons, en appliquant une fois de plus le lemme 1 :

$$(4.7) \quad f(g_p(x),g_p(y)) \equiv f\Big(\sum_{j=0}^{i-1} \lambda_j x^{p^h+j}, \sum_{j=0}^{i-1} \lambda_j y^{p^h+j}\Big) + \lambda_i (x^{p^h+i} + y^{p^h+i}) \pmod{\deg.(p^h+i+1)}.$$

$$(4.8) \quad g_p(f(x,y)) \equiv \sum_{j=0}^{i-1} \lambda_j (f(x,y))^{p^h+j} + \lambda_i (x+y)^{p^h+i} \pmod{\deg.(p^h+i+1)}.$$

Remarquons que la puissance p^h-ième d'une série formelle en x et y est une série formelle en x^{p^h} et y^{p^h} ; si nous appliquons (4.4) en tenant compte de notre hypothèse de récurrence, il vient :

$$(4.9) \qquad \lambda_i B_{p^h+i}(x,y) = k(x^{p^h}, y^{p^h}),$$

où $k(x,y)$ désigne un polynome en x et y. D'après (3.2), si $i \not\equiv 0 \pmod{p^h}$, cette dernière relation implique $\lambda_i = 0$. Ainsi $\lambda_i = 0$ quel que soit $i \not\equiv 0 \pmod{p^h}$, et le lemme 5 est démontré.

<u>Lemme 6</u>. Soient $f(x,y)$ et $f'(x,y)$ deux lois de groupes abéliennes à coefficients dans l'anneau K de caractéristique p, et $g_n(x)$, $g'_n(x)$ leurs n-ièmes itérés respectifs. Alors la relation :

$$f(x,y) \equiv f'(x,y) + aC_{p^h}(x,y) \pmod{\deg.(p^h+1)},$$

où $a \in K$, h entier > 0, implique :

$$g_p(x) \equiv g'_p(x) - ax^{p^h} \pmod{\deg.(p^h+1)}.$$

<u>Démonstration</u>. Nous allons établir plus généralement, par récurrence sur n, les relations :

(4.10) $$g_n(x) = g'_n(x) + a\,\frac{n^{p^h} - n}{p}\,x \qquad (\text{mod.deg.}(p^h+1)).$$ (1)

Cette relation est évidemment exacte pour $n = 1$. Si nous la supposons vraie pour l'entier n, nous avons successivement :

(4.11) $$g_{n+1}(x) = f(x,g_n(x)) \equiv f'(x,g_n(x)) + aC_{p^h}(x,g_n(x)) \quad (\text{mod.deg.}(p^h+1)),$$

(4.12) $$aC_{p^h}(x,g_n(x)) \equiv aC_{p^h}(x,nx) = a\frac{(n+1)p^h - np^h - 1}{p}\,x^{p^h} \qquad (\text{mod.deg.}(p^h+1))$$

(4.13) $$f'(x,g_n(x)) \equiv f'(x,g'_n(x) + a\frac{n^{p^h}-n}{p}\,x^{p^h})$$
$$\equiv f'(x,g'_n(x)) + a\frac{n^{p^h}-n}{p}\,x^{p^h} \qquad (\text{mod.deg.}(p^h+1)).$$

Ces trois dernières relations montrent que (4.10) est vraie pour l'entier $(n+1)$, donc pour tout entier naturel et en particulier pour p, ce qui démontre le lemme 6.

<u>Corollaire 1</u>.- Quel que soit h, il existe une loi de groupe abélienne de hauteur h à coefficients dans l'anneau K de caractéristique p.

En effet, si h est infini, nous prendrons la loi $x+y$. Sinon il nous suffira de prolonger en une loi de groupe (proposition 1) le p^h-bourgeon déterminé par $x + y + C_{p^h}(x,y)$.

<u>Corollaire 2</u>.- Soient $f(x,y)$ et $f'(x,y)$ deux lois de groupe abéliennes à coefficients dans l'anneau K de caractéristique p, $g_p(x)$ et $g'_p(x)$ leurs p-ièmes itérés respectifs, $\varphi(x) \in G_1(K)$ tel que $f^{\varphi} \equiv f'$ (mod.deg. p^h). Alors la relation plus forte $f^{\varphi} \equiv f'$ (mod.deg.(p^h+1)) a lieu si et seulement si $g_p^{\varphi} \equiv g'_p$ (mod.deg.(p^h+1)).

En effet, $f^{\varphi} \equiv f' + aC_{p^h}$ (mod.deg.(p^h+1)), où $a \in K$, et, d'après (4.3) et le lemme 6, la relation $a \equiv 0$ équivaut à $g_p^{\varphi} \equiv g'$ (mod.deg.(p^h+1)).

<u>Proposition 7</u>. La condition nécessaire et suffisante pour qu'une loi de groupe abélienne à coefficients dans l'anneau K de caractéristique p soit équivalente (au sens faible) à la loi $x+y$ est qu'elle soit de hauteur infinie.

<u>Démonstration</u>. La condition est évidemment nécessaire, puisque le p-ième itéré de la loi $x+y$, ainsi que de toutes ses transmutées, est nul. Elle est suffisante d'après la proposition 6 et le corollaire 2 du lemme 6.

---

(1) Les relations (4.10) sont valables même si K n'est pas de caractèristique p

<u>Lemme 7</u>. Soit $g_p(x) = g(x^{p^h})$ une série formelle en x^{p^h} à coefficients dans l'anneau K de caractéristique p ; on suppose $g(x) \equiv \lambda x$ (mod.deg.2) , $\lambda \in K$. Soient $\varphi_1(x)$ et $\varphi_2(x)$ deux éléments de $G_1(K)$ tels que $\varphi_2(x) \equiv \varphi_1(x) + cx^q$ (mod.deg.(q+1)) , où $c \in K$, q entier > 1 . Alors :

$$g_p^{\varphi_2}(x) \equiv g_p^{\varphi_1}(x) + (\lambda^q c - \lambda c^{p^h})x^{qp^h} \qquad (\text{mod.deg.}(q+1)p^h).$$

<u>Démonstration</u> : Nous avons d'abord (cf.(2.21)) :

$$(4.14) \qquad \varphi_2^{-1}(x) \equiv \varphi_1^{-1}(x) - cx^q \qquad (\text{mod.deg.}(q+1)).$$

D'où, en élevant tous les termes à la puissance p^h :

$$(4.15) \qquad (\varphi_2^{-1}(x))^{p^h} \equiv (\varphi_1^{-1}(x))^{p^h} - c^{p^h} x^{qp^h} \qquad (\text{mod.deg.}(qp^h+1)).$$

Ensuite, d'après le lemme 1 :

$$(4.16) \qquad g_p(\varphi_2^{-1}(x)) = g_p(\varphi_1^{-1}(x)) - \lambda c^{p^h} x^{qp^h} \qquad (\text{mod.deg.}(qp^h+1)).$$

$$(4.17) \qquad g_p^{\varphi_2}(x) \equiv \varphi_2(g_p(\varphi_1^{-1}(x))) - \lambda c^{p^h} x^{qp^h} \qquad (\text{mod.deg.}(qp^h+1)).$$

Puisque $g_p(\varphi_2^{-1}(x)) \equiv \lambda x^{p^h}$ (mod.deg.(qp^h+1)) , nous avons :

$$(4.18) \qquad \varphi_2(g_p(\varphi_1^{-1}(x))) \equiv g_p^{\varphi_1}(x) + c\lambda^q x^{qp^h} \qquad (\text{mod.deg.}(p^h+1)).$$

$$(4.19) \qquad g_p^{\varphi_2}(x) = g_p^{\varphi_1}(x) + (\lambda^q c - \lambda c^{p^h})x^{qp^h} \qquad (\text{mod.deg.}(qp^h+1)).$$

Remarquons enfin qu'une congruence (mod.deg.(qp^h+1)) entre deux séries en x^{p^h} équivaut à une congruence (mod.deg.$(q+1)p^h$), ce qui achève la démonstration du lemme

<u>Corollaire</u>. Avec les notations précédentes, $\varphi_1 \equiv \varphi_2$ (mod.deg.q) implique $g_p^{\varphi_1} = g_p^{\varphi_2}$ (mod.deg.qp^h).

Reprenons le problème de l'équivalence de deux lois de groupes abéliennes f et f' à coefficients dans le même anneau K de caractéristique p. Pour que f et f' soient équivalentes, il faut qu'elles aient même hauteur, car une transmutation conserve l'ordre d'une série formelle (degré minimum des composantes homogènes non nulles). Nous supposerons donc que f et f' ont toutes deux la même hauteur

$h < \infty$ (le cas de la hauteur infinie est élucidé par la proposition 7). Soient g_p , g'_p les p-ièmes itérés respectifs de f et f' : $g_p(x) \equiv \lambda\, x^{p^h}$ (mod.deg.$2p^h$), $g'_p(x) \equiv \lambda' x^{p^h}$ (mod.deg.$2p^h$), où λ , $\lambda' \in K$; $\lambda, \lambda' \neq 0$.

Pour que f et f' soient équivalentes au sens faible, il faut que $\lambda = \lambda'$. En effet, quel que soit $\varphi(x) \in G_1(K)$, $g_p^{\varphi}(x) \equiv \lambda\, x^{p^h}$ (mod.deg.$2p^h$) . Nous supposerons d'abord cette condition satisfaite.

Cherchons à construire $\varphi(x) = x + \sum_{i=2}^{\infty} a_i x^i$, tel que $f^{\varphi} = f'$. Pour abréger, nous appellerons q-section de φ et nous noterons φ_q le polynome $x + \sum_{i=2}^{q} a_i x^i$. Une q-section φ_q d'une transmutation φ de f en f' doit vérifier :

$$(4.20) \qquad f^{\varphi_q} \equiv f' \qquad (\text{mod.deg.}(q+1)).$$

Etant donné une q-section φ_q vérifiant (4.20), nous savons, si $(q+1)$ n'est pas une puissance de p , calculer rationnellement $a_{q+1} \in K$ tel que $\varphi_{q+1}(x) = \varphi_q(x) + a_{q+1} x^{q+1}$ vérifie (4.20), où q est remplacé par $(q+1)$.

Pour des raisons typographiques, nous noterons (trans φ_q). g_p , (trans φ_q).f les transmutés respectifs de g_p et de f par φ_q.

Après avoir déterminé φ_{p^k-1} , nous pourrons calculer a_{p^k} si et seulement si (proposition 6 et corollaire 2 du lemme 6) :

$$(4.21) \qquad (\text{trans } \varphi_{p^k-1}).g_p \equiv g'_p \qquad (\text{mod.deg.}(p^k+1)).$$

Pour $k < h$, (4.21) est vérifiée parce que nous avons supposé f et f' de hauteur h ; pour $k = h$, (4.21) est vérifiée parce que nous avons supposé $\lambda = \lambda'$. Considérons donc le cas où $k > h$. Remarquons que

$$\varphi_{p^k-1} \equiv \varphi_{p^{k-h}} \qquad (\text{mod.deg.}(p^{k-h}+1)) \text{ , et appliquons le}$$

corollaire du lemme 7. Nous obtenons :

$$(4.22) \qquad (\text{trans } \varphi_{p^k-1}).g_p \equiv (\text{trans } \varphi_{p^{k-h}}).g_p \qquad (\text{mod.deg.}(p^k+p^h)).$$

Ainsi seuls les choix des coefficients a_i , pour $2 \leq i \leq p^{k-h}$, décident de la possibilité de calculer ultérieurement le coefficient a_{p^k} . Il ne peut y avoir de choix que dans la détermination de $a_p, a_{p^2}, \ldots, a_{p^k}, \ldots$ mais ces choix, supposés

possibles, ne sont pas arbitraires : le choix de a_p conditionne la détermination de $a_{p^{k+1}}$, etc ...

C'est pour cette raison que nous avons mentionné, dans l'introduction, un problème d' "obstruction retardée".

Supposons choisis les coefficients $a_i (2 \leq i \leq p^{k-1})$ de $\varphi_{p^{k-1}}$ de telle sorte que :

$$(4.23) \qquad (\text{trans } \varphi_{p^{k-1}}).g \equiv g'_p \qquad (\text{mod.deg.}(p^{k+h-1}+p^h)).$$

Nous déterminerons ensuite, par des calculs rationnels, les coefficients $a_i \in K$ pour $p^{k-1} < i < p^k$, de façon à obtenir la (p^k-1)-section φ_{p^k-1} vérifiant :

$$(4.24) \qquad (\text{trans } \varphi_{p^k-1}).f \equiv f' \qquad (\text{mod.deg.}p^k).$$

D'après (4.23), nous pourrions déterminer des coefficients $b_i \in K$ de telle sorte qu'en posant : $\Psi(x) = \varphi_{p^k-1}(x) + \sum_{i=p^k}^{p^{k+h}-1} b_i x^i$, on ait :

$$(4.25) \qquad (\text{trans } \Psi).f \equiv f' \qquad (\text{mod.deg.}p^{k+h}),$$

et, par conséquent :

$$(4.26) \qquad (\text{trans } \Psi).g_p \equiv g'_p \qquad (\text{mod.deg.}p^{k+h}).$$

Puisque $\varphi_{p^k-1} \equiv \Psi$ (mod.deg.p^k), le corollaire du lemme 7 donne :

$$(4.27) \qquad (\text{trans } \varphi_{p^k-1}).g_p \equiv (\text{trans } \Psi).g_p \equiv g'_p \qquad (\text{mod.deg.}p^{k+h}).$$

Soit $\mu_k \in K$, tel que :

$$(4.28) \qquad (\text{trans } \varphi_{p^k-1}).g_p(x) = g'_p(x) + \mu_k x^{p^{k+h}} \qquad (\text{mod.deg.}(p^{k+h}+p^h)).$$

Le lemme 7 nous donne alors la condition pour que

$\varphi_{p^k}(x) = \varphi_{p^{k-1}}(x) + a_{p^k} x^{p^k}$ vérifie : $(\text{trans } \varphi_{p^k}).g_p = g'_p \pmod{\text{deg.}(p^{k+h}+p^h)}$.
Il faut et il suffit pour cela que :

$$(4.29) \qquad \lambda\, a_{p^k}^{p^h} - \lambda^{p^k} a_{p^k} = \mu_k .$$

Pour la première fois, nous rencontrerons une équation algébrique non linéaire pour déterminer un élément de K. Cette circonstance nous conduit à prendre comme anneau de base un corps de caractéristique p algébriquement clos.

<u>Théorème 3</u>.- Deux lois de groupes à coefficients dans un même corps K de caractéristique p algébriquement clos sont équivalentes si et seulement si elles ont même hauteur.

<u>Démonstration</u>. Nous savons que la condition est nécessaire, et qu'elle est suffisante dans le cas de la hauteur infinie. Montrons qu'elle est suffisante pour deux lois de groupes f et f' de même hauteur $h < \infty$. Soient, en conservant les notations précédentes, les p-ièmes itérés :
$g_p(x) \equiv \lambda x^{p^h} \pmod{\text{deg.}2p^h}$, $g'_p(x) \equiv \lambda' x^{p^h} \pmod{\text{deg.}2p^h}$, avec $\lambda, \lambda' \in K$, $\lambda, \lambda' \neq 0$.

Transmutons f par $\Psi(x) = ax$, où $a \in K$, $a \neq 0$. Nous avons :

$f^{\Psi}(x,y) = af(a^{-1}x, a^{-1}y)$ et $g_p^{\Psi}(x) = ag_p(a^{-1}x) = a^{1-p^h} \lambda x^{p^h} \pmod{\text{deg.}2p^h}$. Pour que $g_p^{\Psi} \equiv g'_p \pmod{\text{deg.}2p^h}$, il faut et il suffit que :

$$(4.30) \qquad \lambda' a^{p^h-1} = \lambda .$$

Cette équation en a possède (p^h-1) racines distinctes dans K. On les obtient toutes en multipliant l'une d'elles par tous les éléments non nuls du champ de Galois F_{p^h} à p^h éléments, qui est contenu dans le corps algébriquement clos K.

Transmutons donc f par $\Psi(x) = ax$, où a est racine de (4.30). Nous sommes ramenés à l'étude précédente, où nous avons considéré l'équivalence (au sens faible) de lois telles que f^{Ψ} et f', dont les p-ièmes itérés sont congrus $\pmod{\text{deg.}2p^h}$. Nous avons vu que le problème se ramène à la résolution d'une suite d'équations du type (4.29), pour $k=1,2,\ldots$ Or chaque équation (4.29) en a_{p^k} admet p^h racines distinctes dans K. On les obtient toutes en <u>additionnant</u> à l'une d'elles tous les éléments de F_{p^h}, multipliés au préalable par une racine ρ de

l'équation $\rho^{p^h-1} = \lambda^{p^k-1}$. Ainsi la construction de $\varphi(x) \in G_1(K)$ tel que $(f^{\psi})^{\varphi} = f'$ peut se poursuivre "en évitant les obstacles", et $f^{\varphi\circ\psi} = f'$, ce qui démontre le théorème.

Le théorème 3 et le corollaire 1 du lemme 6 montrent qu'il existe une <u>infinité dénombrable</u> de classes de lois de groupes à coefficients dans un corps K de caractéristique p algébriquement clos. En fait, nous ne savons écrire explicitement un représentant que pour deux de ces classes : la loi $x+y$ ("addition"), de hauteur infinie, et la loi $x+y+xy$ ("multiplication"), de hauteur 1 (car son p-ième itéré est x^p).

Une loi de groupe de hauteur h $(1 < h < \infty)$ ne peut pas être un polynome. Soit en effet $P(x,y) \in K[x,y]$ un polynome de degré $\alpha > 1$ en x. Alors $P(P(x,y),z)$ est de degré α^2 en x, tandis que $P(x,P(y,z))$ est seulement de degré α en x. Un polynome ne peut donc être une loi de groupe que s'il est de la forme $x + y + axy$ $(a \in K)$, et, par conséquent, équivalent à $x+y$ ou $x+y+xy$.

La transmutation la plus générale d'une loi de groupe f en une loi de groupe équivalente f' s'écrit sous la forme $\varphi \circ \psi$, où φ est une transmutation particulière de f en f', et ψ un élément quelconque du <u>stabilisateur</u> de f. Si $\mathcal{S}$ désigne le stabilisateur de f, le stabilisateur $\mathcal{S}'$ de f' est : $\varphi \circ \mathcal{S} \circ \varphi^{-1}$. Par conséquent les stabilisateurs des lois de groupes de même hauteur à coefficients dans un même corps K de caractéristique p algébriquement clos sont des sous-groupes conjugués de $G(K)$.

Désignons généralement par $G_i(K)$ l'ensemble des éléments $\varphi(x) \in G(K)$ tels que $\varphi(x) \equiv x \pmod{\deg.(i+1)}$; cette définition, valable pour i entier > 0, contient comme cas particulier la définition du sous-groupe $G_1(K)$ de $G(K)$.

Nous savons déjà (cf.(2.21))que les $G_i(K)$ forment une suite décroissante de sous-groupes dans $G(K)$. Plus précisément, on peut démontrer facilement que les $G_i(K)$ constituent une N-suite dans $G_1(K)$, c'est-à-dire que le commutateur de deux éléments choisis respectivement dans $G_i(K)$ et $G_j(K)$ appartient à $G_{i+j}(K)$, pour tout couple d'entiers $i,j \geqslant 1$.

Le groupe $G(K)/G_1(K)$ s'identifie au groupe multiplicatif K^* de K, en associant à la classe (mod. $G_1(K)$) de $\varphi(x) \in G(K)$ l'élément $a \in K^*$ tel que $\varphi(x) \equiv ax \pmod{\deg.2}$. Le groupe $G_i(K)/G_{i+1}(K)$ s'identifie au groupe additif K, en associant à la classe (mod. $G_{i+1}(K)$) de $\varphi(x) \in G_i(K)$ l'élément $b \in K$ tel que $\varphi(x) \equiv x + bx^{i+1} \pmod{\deg.(i+2)}$.

Si nous prenons sur $G(K)$ la topologie induite par la topologie habituelle

des séries formelles, $G(K)$ devient un groupe topologique complet. Les sous-groupes $G_i(K)$ constituent un système fondamental de voisinages de l'élément neutre dans $G(K)$ qui s'identifie à la limite projective des groupes quotients $G(K)/G_i(K)$, munis de leurs homomorphismes naturels les uns sur les autres.

Si $\mathcal{S}$ désigne le stabilisateur d'une loi de groupe à coefficients dans le corps K, nous poserons $\mathcal{S}_i = \mathcal{S} \cap G_i(K)$, pour tout entier $i \geqslant 1$. Les sous-groupes $\mathcal{S}_i$ constituent un système fondamental de voisinages de l'élément neutre dans le sous-groupe fermé (donc complet) $\mathcal{S}$ de $G(K)$; $\mathcal{S}_1$ est le stabilisateur faible de la loi de groupe. Les groupes quotients $\mathcal{S}/\mathcal{S}_1$ et $\mathcal{S}_i/\mathcal{S}_{i+1}$ s'identifient à des sous-groupes de $G(K)/G_1(K)$ et de $G_i(K)/G_{i+1}(K)$ respectivement, donc aussi à des sous-groupes de K^* et de K, respectivement. Nous utilisons ces identifications canoniques dans l'énoncé de la :

<u>Proposition 8</u>. Si $\mathcal{S}$ est le stabilisateur d'une loi de groupe de hauteur h finie à coefficients dans un corps K de caractéristique p algébriquement clos, et si $(\mathcal{S}_i)$ est la suite de sous-groupes de $\mathcal{S}$ précédemment introduite,

a) $\mathcal{S}/\mathcal{S}_1$ s'identifie à $F_{p^h}^* \subset K^*$; c'est donc un groupe cyclique d'ordre (p^h-1).

b) $\mathcal{S}_{q-1}/\mathcal{S}_q$ s'identifie à l'ensemble $\rho_q F_{p^h}$ des éléments $\rho_q a$ ($\rho_q \in K$, $a \in F_{p^h}$), où :

$\rho_q = 0$ si q n'est pas une puissance de p ;

ρ_q est une racine de l'équation $\rho_q^{p^h-1} = \lambda^{p^k-1}$ (si $q = p^k$), l'élément $\lambda \in K$ étant lié au p-ième itéré g_p de la loi de groupe par la relation $g_p(x) \equiv \lambda x^{p^h}$ (mod.deg.$2p^h$).

<u>Démonstration</u>. La proposition 8 ne fait que traduire, en tenant compte des identifications introduites, les résultats obtenus dans l'étude des transmutations d'une loi f en une loi f', que nous supposons maintenant confondue avec f (cf.(4.29) et (4.30)).

Si la loi considérée était de hauteur infinie, $\mathcal{S}/\mathcal{S}_1$ s'identifierait à K^* et $\mathcal{S}_{q-1}/\mathcal{S}_q$ à K pour q égal à une puissance de p.

Considérons une loi de groupe f à coefficients dans un corps K de caractéristique p (non nécessairement algébriquement clos), et soit K' une extension de K. Nous pouvons, par une identification évidente, considérer que f a ses

coefficients dans K'. Soient $\mathcal{S}$ et $\mathcal{S}'$ les stabilisateurs de f lorsqu'on la considère sur K et K' respectivement. Le stabilisateur $\mathcal{S}$ s'identifie canoniquement à un sous-groupe fermé de $\mathcal{S}'$. Mais, si K est <u>algébriquement clos</u>, et si la hauteur h de f est finie, la proposition 8 montre que $\mathcal{S}' = \mathcal{S}\mathcal{S}'_1$ et $\mathcal{S}'_q = \mathcal{S}_q\mathcal{S}'_{q+1}$ pour tout entier q. Autrement dit, $\mathcal{S}$ est dense dans $\mathcal{S}'$, et, comme $\mathcal{S}$ est fermé, $\mathcal{S} = \mathcal{S}'$. Ainsi le stabilisateur d'une loi de groupe de hauteur finie à coefficients dans un corps K de caractéristique p algébriquement clos est invariant par toute extension de K. La proposition 8 montre de plus que c'est un groupe <u>compact</u>, limite projective des groupes finis $\mathcal{S}/\mathcal{S}_i$. Nous pouvons donc énoncer la :

<u>Proposition 9</u>. Le stabilisateur d'une loi de groupe de hauteur finie à coefficients dans un corps de caractéristique p est un groupe <u>compact</u>. Les stabilisateurs de deux lois de groupes de même hauteur finie à coefficients dans deux corps de caractéristique p algébriquement clos sont isomorphes.

Nous obtenons donc ainsi une suite infinie de groupes compacts, définis chacun à un isomorphisme près.

Soit f une loi de groupe de hauteur finie h à coefficients dans un corps K de caractéristique p, $\mathcal{S}$ son stabilisateur, et $g_n(x)$ ses n-ièmes itérés. Nous avons :

$$(4.31) \qquad g_p(x) \equiv \lambda\, x^{p^h} \qquad (\text{mod.deg.}2p^h)\ , \text{ avec } \lambda \in K\ ,\ \lambda \neq 0\ .$$

D'après (4.4), (4.5), (4.2) :

$$(4.32) \qquad g_n(x) \in \mathcal{S}\ , \text{ si } n \not\equiv 0 \quad (\text{mod.}p).$$

$$(4.33) \qquad g_{p^k}(x) \equiv \lambda^{\frac{p^{kh}-1}{p^h-1}}\, x^{p^{kh}} \qquad (\text{mod.deg.}(p^{kh} + p^h)).$$

Nous en déduisons, d'après (4.1), que, pour tout entier $k \geqslant 0$:

$$(4.34) \qquad n \equiv n' \quad (\text{mod.}p^k) \quad \text{équivaut à} \quad g_n(x) \equiv g_{n'}(x) \quad (\text{mod.deg.}p^{kh}).$$

Si n tend, au sens de la topologie p-adique, vers un entier p-adique ν, $g_n(x)$ tend, au sens de la topologie des séries formelles, vers une série déterminée $g_\nu(x)$.

La relation (4.34), ainsi que les relations (4.1) à (4.5), restent valables lorsque les entiers rationnels n et n' y sont remplacés par des entiers p-adiques. Par conséquent, si $\nu \not\equiv 0 \pmod{p}$, $g_\nu(x) \in \mathcal{S}$, et $g_\nu^{\varphi} = g_\nu$, pour tout $\varphi \in \mathcal{S}$.

Si nous désignons par Z_p^* le groupe multiplicatif des unités p-adiques (entiers p-adiques inversibles), l'application : $\nu \to g_\nu(x)$ est un isomorphisme (et un homéomorphisme) de Z_p^* sur un <u>sous-groupe fermé central</u> (c'est-à-dire contenu dans le centre) du stabilisateur $\mathcal{S}$. Nous appellerons ce sous-groupe : <u>groupe des itérés p-adiques</u>.

<u>Proposition 10</u>. Le stabilisateur d'une loi de groupe de hauteur 1 à coefficients dans un corps de caractéristique p coïncide avec le groupe des itérés p-adiques.

<u>Démonstration</u>. Faisons, éventuellement, une extension du corps de base pour obtenir un corps algébriquement clos. Désignons par $\mathcal{S}$ le stabilisateur, par $\mathcal{S}'$ le groupe des itérés p-adiques, qui reste invariant par l'extension, et posons, pour tout entier $i \geqslant 1$, $\mathcal{S}'_i = \mathcal{S}' \cap \mathcal{S}_i$. La relation (4.33), où il faut remplacer h par 1, montre que $\mathcal{S}'/\mathcal{S}'_1$ est un groupe cyclique d'ordre $(p-1)$ et que $\mathcal{S}'_{q-1}/\mathcal{S}'_q$ est un groupe cyclique d'ordre p si q est une puissance de p. Si nous appliquons la proposition 8, nous voyons que $\mathcal{S}'$ est dense dans $\mathcal{S}$. Comme $\mathcal{S}'$ est fermé, $\mathcal{S} = \mathcal{S}'$, et l'extension du corps de base a laissé invariant le stabilisateur $\mathcal{S}$.

Il serait souhaitable d'étudier les stabilisateurs des lois de groupes de hauteur h $(1 < h < \infty)$ sur un corps de caractéristique p algébriquement clos. Ces groupes sont toujours <u>non-abéliens</u>. En effet, si nous étudions une loi de groupe de hauteur $h > 1$, nous pouvons toujours supposer, après remplacement éventuel par une loi équivalente, que $f(x,y) = x + y \pmod{\deg. p^2}$, et que le p-ième itéré g_p de f vérifie : $g_p(x) = x^{p^h} \pmod{\deg. 2p^h}$. Montrons, avec les notations précédentes, que $\mathcal{S}_{p-1}/\mathcal{S}_{p^3-1}$ n'est pas abélien. Pour tout $a \in F_{p^h}$, nous pouvons prolonger $x + ax^p$ en une série $\varphi(x) \in \mathcal{S}$, telle que $\varphi(x) \equiv x+ax^p+bx^{p^2} \pmod{\deg.(p^2+1)}$ où $b \in K$. Soit $\varphi'(x) \equiv x+a'x^p+b'x^{p^2} \pmod{\deg.(p^2+1)}$ un autre élément de $\mathcal{S}$. Alors

$$\varphi \circ \varphi'(x) \equiv x+(a+a')x^p+(b+b'+aa'^p)x^{p^2} \pmod{\deg.(p^2+1)}, \text{ et}$$

$$\varphi \circ \varphi(x) \equiv x+(a'+a)x^p+(b'+b+a'a^p)x^{p^2} \pmod{\deg.(p^2+1)}.$$ Puisque a et a' peuvent être choisis quelconques dans $F_{p^h} \supset F_{p^2}$, nous pouvons supposer que

$aa'^p \neq a'a^p$, ce qui prouve que $\mathcal{S}_{p-1}/\mathcal{S}_{p^3-1}$ n'est pas abélien.

Il existe des lois de hauteur h telles que les séries appartenant au stabilisateur correspondant aient tous leurs coefficients dans F_{p^h}. Partons en effet d'une loi $f(x,y)$ de hauteur h à coefficients dans un corps K de caractéristique p algébriquement clos, et soit $g_p(x)$ son p-ième itéré. En appliquant le lemme 7, nous démontrons facilement qu'il existe $\varphi(x) \in G(K)$ tel que $g_p^{\varphi}(x) = x^{p^h}$. Si $\Psi(x) = \sum_{i=1}^{\infty} a_i x^i$ est un élément du stabilisateur de f^{φ}, nous devons avoir $\Psi(x^{p^h}) = (\Psi(x))^{p^h}$, condition équivalente à $a_i \in F_{p^h}$ pour tout $i \geqslant 1$.